RESEARCH ARTICLE OPEN ACCESS

Secured Remote Network Architecture with Gateway Server

Tarun Vasagiri
MTech Student, Dept. of CSE, MIT, Manipal

ABSTRACT

Network security is a paramount concern for many organisations which are recently started adopting work from home culture on a large scale. This sudden shift to remote work environment during COVID pandemic times, made many small and medium scale companies vulnerable to multiple cyber attacks. During the COVID pandemic times, the number of such attacks increased by 600%. It is high time and every organization is looking for security solutions on all levels. This research tries to develop a holistic network model to enable organisations facilitate remote access to the network while handling the major security threats.

Keywords: -Network Security, Cloud Security, Secured Network Architecture, Firewall, Proxy

I. INTRODUCTION

DURING the COVID pandemic, majority of the organisations to work from home culture than before. According to Global Workplace Analytics forecast, 25-30% of the U.S. workforce will be working-from-home one or more days a week after the pandemic. This sudden increase in the work from home culture put a lot of pressure on the organisations to facilitate remote work. Big and well-developed organisations were able to adopt this change easily as they already have resources and are used to employees working form home time to time but, many other organisations were either paying a lot for money for some third party resources or becoming vulnerable to many cyber attacks by implementing faulty and less secured remote environments. Gartner insight projected that businesses would spend more than $123 billion on security in 2020 and projects that figure to grow to $170.4 billion by 2022. [5] Even after such huge investments, they cyber attacks peaked during the same time. The use of malware increased by 358% through 2020, and ransomware usage increased by 435% compared to the previous year, according to a study by Deep Instinct. July 2020 alone saw a 653% increase in malicious activity compared to the same month in 2019. [6] Such organisations need a low cost network architecture which is capable enough of handling the general functionalities of the remote network and provides enough security to handle major security vulnerabilities.

II. CLOUD AND SECURITY ISSUES

Cloud network is a group of virtual network nodes hosted in a data centre provided by service providers or managed in-house and are available on demand. These network nodes can include virtual routers, load balancers, firewalls, and network management software, with other tools and functions available as required.

Majority of the organizations use more than one kind of network. Few of their resources will be on cloud and a few on premise resources or a private cloud. Such a network setup is called a hybrid network. Though both on premise and cloud networks are well secured individually, the vulnerability arises when one network tries to communicate with the other. But this hybrid network can be expensive and opens the network to multiple security vulnerabilities.

• *Tarun V is with the Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal, India, 576104. E-mail: tarunvasagiri98@gmail.com*

III. RESEARCH METHODOLOGY

This article describes a network model which is capable enough to mitigate the current security threats. In order to achieve it, the list of current security threats are identified by extensive research on recent cyber attacks on networks and organizations, cloud resources and attack trends. Most accepted convention in providing network security is by providing confidentiality, authentication and integrity. [1] approach sticks to the above mentioned conventions and their model implements backward compatibility that might aid in replacing password-based mechanisms eventually in the future. [1] also leaves with numerous insights for research consisting of quantifying the efficacy of the proxy gateway in a network architecture taking various other scenarios in accounts. [2] discussed the necessity of encryption mechanism to provide confidentiality and integrity in detail by implementing a hybrid encryption mechanism. Idea of encryption is taken from [2] and replaced the hybrid encryption with AES encryption in this paper as a part of mitigation methods discussed below.

After the concerned threats are identified, study is done on several mitigation methods and their implementation costs. With this information, in this paper a network model is designed using multiple kinds of low cost and effective mitigation methods in order to provide complete protection from all identified attacks during the course of study.

IV. ATTACK TRENDS

A cyber attack is an effort or trail to perform any unauthorised activity on the network as whole or a network node with a malicious intent. The purposes can

include breaching data, stealing information or breaking a resource

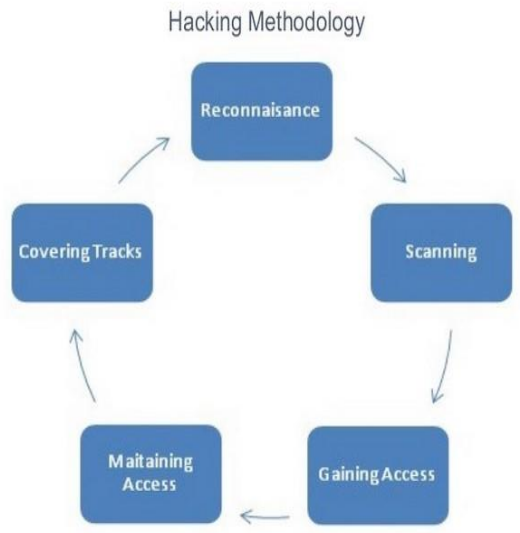

Fig. 1. Hacking Methodology.

down. The attacks are performed by a process called attack methodology. It consists of five major steps: [Refer fig 1]

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Covering Tracks

The most important and first step is Reconnaissance. This step is responsible for detecting the vulnerabilities which are exploited in later steps of hacking methodology. It is performed in 6 steps:

1. Gathering Information
2. Network Range Determination
3. Active machine identification
4. Port scan and Host scan
5. OS Fingerprinting
6. Network Mapping

IV.1 Attacks Identified

Consider a hypothetical scale of security, closing the network down so that no one can access it at left end of the scale and opening the network for everyone without restrictions on the right end. Choosing the left-most point on the scale which meets all the requirements of the network is called security. Any network with such security implemented is called a secured network.

On a broader terms, the attacks are classified into two types: *Active* and *Passive* [6]

Passive attacks are those attacks where interception and monitoring of data alone takes place. Release of message content and traffic analysis are two types of passive attacks.

Active attacks are those attacks where the data is modified or fabricated. Masquerade, Reply, Modification and DoS are a few types of active attacks.

Some of the common types of network attacks are listed below: [7]

TABLE 1
Attacks and Descriptions. [5]

ATTACK	DESCRIPTION
Man in the Mid-dle Attack	Attacker can modify and intercept communications and deploy third party involvement.
Smurf Attack	Attacker uses spoofed IP addresses for purpose of hiding the identity to generate flooded with traffic at the victim machine.
Denial of Service	DoS attacks try to render web service unavailable to users.
Side-Channel Attacks	Attacker gains information about the cryptographic technique.
Viruses and Worms	Attacker may use certain bad source code to compromise.
Tampering with data	An attacker may modify or fabricate information.
Cloud Malware Injection attack	Attacker inject implement of a maliciously service in cloud

1. Reconnaissance Attacks - Packet Sniffers, Port Scan, PingSweep, Internet Information Queries.
2. Password Attacks - Brute Force, Key Loggers and Phishing.
3. Man-in-the-middle Attacks.
4. Denial of Services - DDoS, Buffer Overflow and SocketOverflow.
5. Malware and Virus.
6. SQL Injection.
7. Social Engineering.

IV.2 Vulnerabilities

Vulnerabilities are the flaws or weaknesses in the system architecture and design which acts like point of failures in case of cyber attack. Attackers first try to find these vulnerabilities and then equip themselves with tools and attacks to exploit them. Every cyber attack that is performed needs a vulnerability which is exposed during reconnaissance. Each type of attack listed in the section above also have a set of vulnerabilities

responsible. The mapping of the identified attacks with their vulnerabilities is listed in Table 2

4.2.1 Classification of Attacks

Based on the vulnerability type, the attacks can be classified into three types: 1. Interference Based
2. Server Based
3. Service Based

Interference Based attacks are based on the vulnerabilities like plain text traffic, weak encryption, etc. This type covers a range of attacks like man-in-the-middle, sniffing, packet hijacking and other similar attacks.

Server Based attacks are possible because of weak security policies in organisations. When servers are improperly configured with no or incomplete OS hardening policies and weak firewall configurations, servers are prone to such attacks. Majority of such attacks are performed by using

TABLE 2
Attacks and Vulnerabilities.

ATTACK	VULNERABILITIES
Reconnaissance Attacks	1) Improper firewall configurations 2) Improper signature handling 3) Commutation in plan text format
Password Attacks	1) No complex passwords 2) Lack of cyber security awareness
Man in the Mid-dle attacks	1) Plain text traffic 2) Weak encryption algorithms 3) Improper key handling
Denial of Services	1) Weak firewall configurations 2) Improper OS configurations
Malware and Virus	1) Weak organisation security 2) policy Weak end point security
SQL Injection	1) Improper coding practices 2) Poor QA
Social Engineering	1) Lack of cyber security awareness 2) Weak organisation security policy

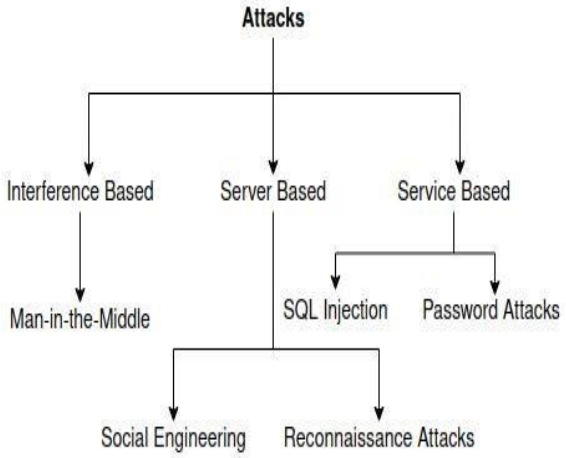

Fig. 2. Attack Classification.

reconnaissance tools and these attacks are on the machine level and not related to any application.

Service Based attacks are based on the application vulnerabilities like insecure coding, poor application architecture, uninstalled patches, etc. These attacks are performed by exploiting the applications and escalating through them.

V. MITIGATION METHODS

Each of the classified attack type needs to be addressed individually and such mitigation methods must be integrated to provide a holistic security model.

V.1 Mitigating Interference based Attacks

Interference attacks are majorly depended in the ability of the attacker to understand the traffic or the inability of the network to hide its traffic. The following techniques can be implemented to prevent such attacks:
1. HTTPS needs to be implemented
2. Authentication like Public Key Pair Based
3. VPN or Virtual Private Network
4. Traffic Encryption
5. Strong router credentials

V.2 Mitigating Server based Attacks

Mitigating attacks on server hardware and resources requires a combination of policies, physical security and OS hardening. Aggressive organisational policies must be introduced restricting the personnel access to the machines. Every machine must have OS hardening performed which must aim to permanently remove all

the unused applications on the machine including the OS level applications. In order to achieve this, air tight classification of resources must be done into groups based on the utilisation of their hardware and each group must have a tailored group policy to handle them. Group of firewalls must be installed handling different scopes like perimeter firewall to handle the traffic between the organisation and the internet on a global level, network firewall to handle the traffic internally between multiple networks inside the organisation. Honey pots and Gateway VMs are the few of the best techniques that can be implemented in this regard.

V.3 Mitigating Service based Attacks

Vulnerabilities of services are highly dynamic in nature and new vulnerabilities are created every time an application introduces new features. It is impractical to create in-house solutions for every requirement. Handling such threats requires out of box implementations which can provide a blanket protection or at least minimisation against attacks on all kinds of applications and vulnerabilities. Prevention of such attacks requires a process instead of a plug and play applications. Every application that is installed in the network must be scrutinised and the traffic pattern must be analysed - what kind of traffic to and fro the applications is supposed to happen in a healthy situation. Based on this understanding appropriate policy changes must be done on the packet-filters. Smart packet filters and network monitors powered with ML must be installed on gateways to detect any malicious activity in the traffic.

VI. SECURED NETWORK MODEL

In the identified mitigation techniques, considering performance constant, there are two major factors which needs to be considered - redundancy and cost. Redundancy is observed when two mitigation techniques have some functionalities in common or both of them does same work. For example, an endpoint security provides protection against malware attacks on computer by setting up a packetfiltering firewall along with its other features; a network level firewall also provides packet-filtering mechanism on a

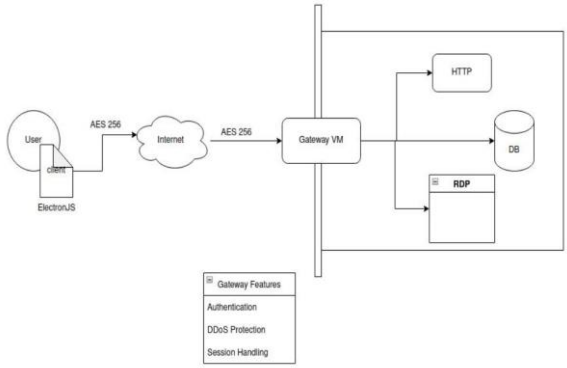

Fig. 3. Designed Model.

greater scope. In such situation both the mitigation methods are doing the same job which is a waste of computational resources. Cost must be managed by considering how much one has to pay for a particular mechanism in one mitigation technique and compare it with other possibilities. For example, in the earlier scenario, cost of packet-filtering mechanism in endpoint security solution and network firewall must be enquired and decision has to be made accordingly.

VI.1 Designed Model

This model has three parts - User End, Gateway VM and Secured Network.

User End is an installable application which handles the user machine security. It has three important functionalities:

1. Machine Checks
2. Usage Monitoring
3. Encryption
4. Authentication

Machine checks are a series of security validations which runs a thorough scan for malwares, checks for updates of OS and default applications, etc. These must be done once during the installation of user-end application and make the system ready to be associated with the network. Usage monitoring is to be started with boot everytime after the user-end application is installed. It is supposed to monitor the Network activity on the users machine and uses a ML algorithm to analyse the activity and detect abnormality. The entire traffic from the user machine to the gateway VM must be encrypted using AES-256 bit algorithm which is handled by the user-end application before sending the traffic from the computer to gateway. It is also responsible for decryption of the traffic that it receives from the gateway VM using the same algorithm. It acts as the front-end for authentication, user enters the credentials in the application which are validated by the Gateway VM.

Gateway VM acts as the one and the only source of traffic to the Secured Network. It receives traffic from multiple userend applications and it forwards the traffic to the destination inside the network only after the user-end application is authenticated. It acts like a two way proxy and hides the identity of the original server from the internet. Anti-DoS setup must be made on the gateway VM to prevent failure as it may be single point of failure in case of attacks. Preferably High Availability architecture is advised on this Gateway.

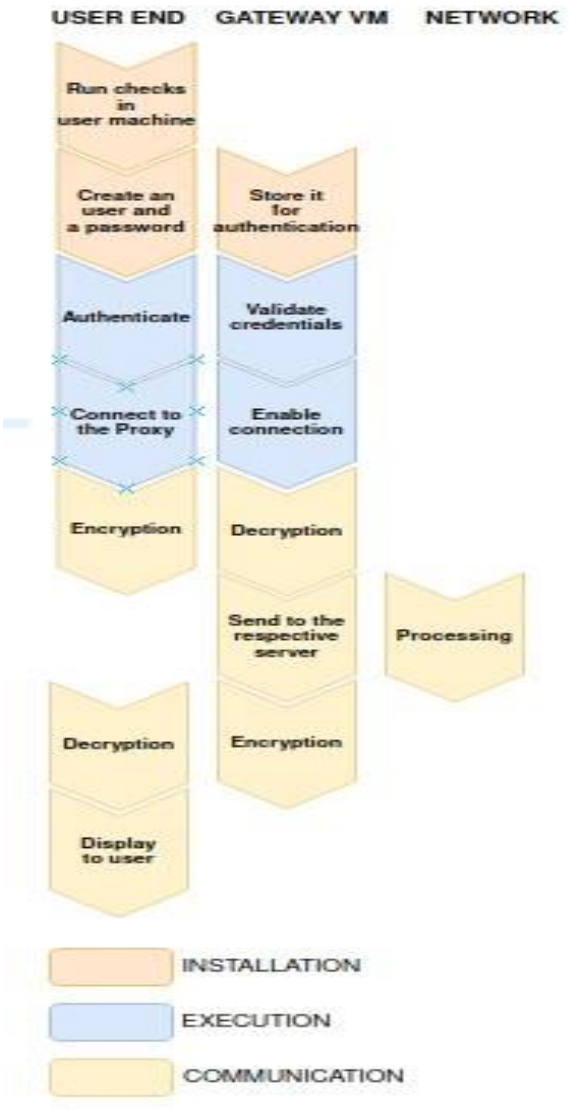

Fig. 4. Work Flow in designed model.

Secured Network refers to the organisation network of original servers which are cut-off from internet and only communicates with the Gateway. It has a set of firewalls - Perimeter firewall to block traffic from internet, Network firewall to create DMZ inside the network and Machine level firewalls on the servers to prevent unwanted applications to be available on the network.

VII. CONCLUSION

The workflow diagram descries in detail the expected flow of traffic in the designed model. Considering the pace with which the cyber attacks are increasing in the market, lowcost efficient security solutions are in great demand. Any such security solutions defends the cyber space on technical level but another important factor which is one of the major reasons for attacks is the awareness among the users. Social engineering attacks are targets the emotional space in information technology which is vulnerable because of lack of knowledge on such attacks. Organisations need to organise multiple seminars, workshops and training programs to enlighten their employees and users on the cyber attacks.

ACKNOWLEDGMENTS

The author would like to thank Mr C Ganesh Babu and Mr Manamohana Krishna, Asst. Professors in the Department of Computer Science, Manipal Institute of Technology, Manipal, India for Their valuable guidance in this research and for mentoring during the course of this research.

REFERENCES

[1] L. F. B. Soares, D. A. B. Fernandes, M. M. Freire and P. R. M. Inacio, ”Secure user authentication in cloud computing manage-´ ment interfaces,” 2013 IEEE 32nd International Performance Computing and Communications Conference (IPCCC), 2013, pp. 1-2, doi: 10.1109/PCCC.2013.6742763.

[2] N. Gajra, S. S. Khan and P. Rane, ”Private cloud security: Secured user authentication by using enhanced hybrid algorithm,” 2014 International Conference on Advances in Communication and Computing Technologies (ICACACT 2014), 2014, pp. 1-6, doi: 10.1109/EIC.2015.7230712.

[3] Work-at-Home After Covid-19 – Our Forecast https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast

[4] Cybersecurity Statistics https://www.fortinet.com/resources/cyberglossary/cyb statistics

[5] A Review on Security Issues and their Impact on Hybrid Cloud Computing Environment - *Mohsin Raza* International Journal of Advanced Computer Science and Applications, Vol. 10, No. 3, 2019

[6] Analysis of Network Security Threats and Vulnerabilities by Development Implementation of a Security Network Monitoring Solution - *Nadeem Ahmad* Master's Thesis ,Sept 2010

[7] Vulnerabilities in Network Infrastructures and Prevention/Containment Measures - *Oludele Awodele* Proceedings of Informing Science IT Education Conference (InSITE) 2012

[8] Method and System for Providing Cloud Based Network Security Services *Juzer Kopti* April 2014

[9] Technical Report on Cloud Security *Aisha Muhammad* January 2021

[10] Top 10 OWASP attacks, vulnerability scanning and exploitation *https://owasp.org/*

[11] Article on Ethical Hacking and Methodologies *https://medium.com/@DianApps/ethical-hacking-and-its-methodology-41468bc2ea67*

[12] Article on Network Models *https://www.section.io/engineeringeducation/networking-models-introductory-guide/*

[13] Article on Proxies *https://www.jscape.com/blog/bid/87783/forwardproxy-vs-reverse-proxy*

[14] Article on Firewalls *https://bts-consulting.biz/2017/10/11/the-threedifferent-types-of-firewalls/*

[15] RFC3826 *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*